Vereinbarung zur Auftragsdatenverarbeitung gemäß Art. 28 DS-GVO

zwischen

.....

APOTHEKE (- Auftraggeber -)

-Apothekenstempel-

und

.....

Lofarma Deutschland GmbH
Hanns-Martin-Schleyer-Str. 26
47877 Willich
vertreten durch
Paesel + Lorei GmbH & Co. KG
Nordring 11
47495 Rheinberg

-Auftragnehmer-

.....

1. Gegenstand und Dauer des Auftrags

(1) Der Auftraggeber bestellt patientenindividuell herzustellende Arzneimittel unter Angabe folgender personenbezogener Daten der Patienten: Name, Vorname, Geburtsdatum, Krankenversicherung der Patienten sowie die Bezeichnung und Zusammensetzung des bestellten Arzneimittels.

(2) Bei der Bestellbearbeitung verarbeitet der Auftragnehmer die personenbezogenen Daten für den Auftraggeber. Die Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union statt.

(3) Die Verarbeitung beginnt am 01.05.2018 und erfolgt auf unbestimmte Zeit bis zur Kündigung dieses Vertrags.

2. Technisch-organisatorische Maßnahmen

Der Auftragnehmer dokumentiert die Umsetzung der in der **Anlage 1** genannten technischen und organisatorischen Maßnahmen. Er darf alternative adäquate Maßnahmen umsetzen. Wesentliche Änderungen sind zu dokumentieren.

3. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die zu verarbeitenden Daten nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst und arzneimittelrechtlich und steuerrechtlich möglich, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer gewährleistet die Einhaltung der gesetzlichen Pflichten gemäß Art. 28 bis 33 DS-GVO durch

a. die Bestellung eines Datenschutzbeauftragten, dessen aktuelle Kontaktdaten auf der Homepage des Auftragnehmers hinterlegt sind;

b. den Einsatz von Beschäftigten ein, die auf Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf die Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse;

c. die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde beim Auftragnehmer, soweit sie sich auf diesen Auftrag beziehen;

d. die Unterstützung des Auftraggebers bei Kontrollen der Aufsichtsbehörde beim Auftraggeber, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer;

e. regelmäßige Kontrolle der internen Prozesse sowie der technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

5. Unterauftragsverhältnisse

(1) Der Auftragnehmer darf Unterauftragnehmer nur mit Zustimmung des Auftraggebers in Textform beauftragen. Der Auftragnehmer wird alle bereits zum Vertragsschluss bestehenden Unterauftragsverhältnisse in der **Anlage 2** zu diesem Vertrag angeben.

(2) Nicht als Unterauftragsverhältnisse gelten Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

6. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber darf im Benehmen mit dem Auftragnehmer die Einhaltung der gesetzlichen und vertraglichen Vorschriften zum Datenschutz im erforderlichen Umfang kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunft verpflichtet, soweit dies zur Durchführung der Kontrolle erforderlich ist.

(3) Für die Ermöglichung von Kontrollen kann der Auftragnehmer eine Aufwandsentschädigung beanspruchen.

7. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen, insbesondere durch

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen;

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Aufwandsentschädigung beanspruchen.

8. Weisungsbefugnis des Auftraggebers

(1) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

9. Löschung und Rückgabe von personenbezogenen Daten

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu vernichten.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

_____

Stephan Kerkojus
Geschäftsführer
Lofarma Deutschland GmbH, Willich

_____

Dr. Anne Pfitzner
Geschäftsführende Gesellschafterin
Paesel + Lorei GmbH & Co. KG, Rheinberg

……, den ……..

_____

Unterschrift, Apotheke

Anlage 1– Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Zutrittskontrolle
  Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
- Zugangskontrolle
  Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- Zugriffskontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
- Trennungskontrolle
  Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Weitergabekontrolle
  Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- Eingabekontrolle
  Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- Verfügbarkeitskontrolle
  Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle
  Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Anlage 2– Unterauftragsverhältnisse

Firma	Anschrift	Leistung
Lofarma SpA	Viale Cassala 40 Milano/Italia	Lohnherstellung
----------	----------	----------